

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-205421

(43) 公開日 平成9年(1997) 8月5日

| (51) Int.Cl. <sup>8</sup> | 識別記号  | 庁内整理番号   | F I           | 技術表示箇所  |
|---------------------------|-------|----------|---------------|---------|
| H 0 4 L 9/18              |       |          | H 0 4 L 9/00  | 6 5 1   |
| G 0 9 C 1/00              | 6 1 0 | 7259-5 J | G 0 9 C 1/00  | 6 1 0 D |
| H 0 4 N 7/167             |       |          | H 0 4 N 7/167 | Z       |

審査請求 未請求 請求項の数 3 O L (全 4 頁)

(21) 出願番号 特願平8-12213

(22) 出願日 平成8年(1996) 1月26日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 吉本 雅彦

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

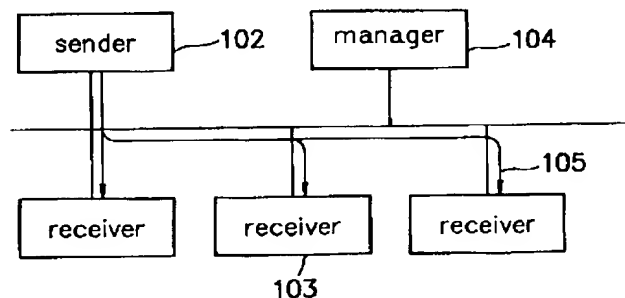
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 データ伝送装置

(57) 【要約】

【課題】 動画データを送信において秘話機能を低コストで実現する。

【解決手段】 送信端末102は送信すべき動画データを伝送単位毎に変換手段を用いて変換した後、コンピュータネットワーク101に送出する。管理端末104は所定の認証手段を用いて上記変換手段を認証して受信端末103に伝達する。受信端末103は認証された変換手段を取得し、これに対応する逆変換手段を構成し、この逆変換手段を用いて受信した変換されたデータを逆変換することにより元の動画データを再生する。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項 1】 送信側においてデータを伝送単位毎に変換する変換手段と、

上記変換手段を認証し、受信側に伝達する認証手段と、受信側において上記認証手段から取得した変換手段に基づいて逆変換手段を構成し、この逆変換手段を用いて上記変換されたデータから元のデータを再生する再生手段とを備えたデータ伝送装置。

【請求項 2】 上記データが可変長符号化方式によって符号化されている場合に、被符号化データの先頭部分だけを別の符号に変換するような伝送単位変換手段を有する請求項 1 記載のデータ伝送装置。

【請求項 3】 上記データが動画データであることを特徴とする請求項 1 記載のデータ伝送装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明はユーザ間またはグループ内での秘話機能を有するデータ伝送装置に関するものである。

## 【0002】

【従来の技術】 近年、ワークステーションやパーソナルコンピュータで利用できる動画コーデックが多数生産されるようになり、これらを用いたテレビ会議システムなどが低価格で提供されるようになってきた。しかしながら、テレビ会議などで必要とされる秘話機能が必ずしも標準的に備わっているとはいえないのが現状である。特に上記のシステムは、従来コンピュータ間のデータ通信に用いられてきた汎用ネットワークを使用する形態のものが主流であり、多くの汎用ネットワークは盗聴の可能性を排除することが困難であることから、何らかの形でデータそのものを保護するような秘話機能が不可欠であった。

## 【0003】

【発明が解決しようとする課題】 上述したデータそのものを保護する方法としては暗号化を適用するのが基本的であって、デジタル署名を用いた電子メールシステムなどの例がある。しかし、動画データは一般に大容量であるため、高性能な暗号化機構を採用する必要があり、システム全体の高コスト化を招くという問題があった。

【0004】 本発明は以上説明した問題を解決するために成されたもので、ネットワークを介して動画データ等の大容量データの通信を行う場合に、データの保護を低コストで実現することを目的とする。

## 【0005】

【課題を解決するための手段】 本発明においては、送信側においてデータを伝送単位毎に変換する変換手段と、上記変換手段を認証し、受信側に伝達する認証手段と、受信側において上記認証手段から取得した変換手段に基づいて逆変換手段を構成し、この逆変換手段を用いて上

記変換されたデータから元のデータを再生する再生手段とを設けている。

## 【0006】

【作用】 本発明によれば、送信側では、データを変換手段により伝送単位毎に変換し、変換されたデータを送信する。受信側では、認証手段で認証されて取得した変換手段に基づいて逆変換手段を構成し、この逆変換手段を用いて受信したデータを逆変換して元のデータを再生する。これによって秘話機能を低コストで実現することができる。

## 【0007】

【発明の実施の形態】 以下、本発明の第 1 の実施の形態について図を用いて説明する。図 1 は本発明による動画送受信システムの構成を示すブロック図である。図において、101 は後述する端末群が接続されるコンピュータネットワークである。102 は動画データの送信端末で、この端末上で稼働するアプリケーション sender によって、動画の取得とネットワークへの送信とが行われる。103 は動画データの受信端末で、この端末上で稼働するアプリケーション receiver によって、ネットワークからの受信と表示あるいは保存等の処理とが行われる。

【0008】 104 は上記 sender や receiver が、相互にデータを交換する上で必要な管理情報を保持する管理端末で、この端末上で稼働するアプリケーション manager によって、上記管理情報の収集と分析、および sender や receiver の一連の制御を行う。なお本実施の形態においては、上記管理情報として後述する伝送単位変換手段を含むものとし、この伝送単位変換手段の取得には信頼できる認証手段が適用されるものとする。105 は上記 sender が送出した動画データの流れを表しており、一般に複数の receiver に対して送られる。なお、以上において各端末毎にアプリケーションが稼働するものとしたが、一般にはこの限りではなく、同一の端末上で任意のアプリケーションが複数個同時に稼働してもよい。

【0009】 図 2 は、sender が動画の送信を行う際の手順を示すフローチャートである。始めに伝送単位変換手段 c を設定する（ステップ S 201）。次に、この伝送単位変換手段 c を manager に登録する（ステップ S 202）。以下、ユーザの指定やファイルの終了検知など、sender が任意に設定した動画データの送信終了検知機構に基づいて送信終了の判定を行い（ステップ S 206）、送信終了でない場合は以下の処理を行う。すなわち、sender が任意に設定した動画データ取得手段を用いて、動画データの取得を行う（ステップ S 203）。次に取得された動画データを伝送単位変換手段 c によって変換する（ステップ S 204）。最後に、上記変換された動画データの送信を行う（ステップ S 205）。

【0010】図3はreceiverが動画像の送信を行う際の手順を示すフローチャートである。始めにmanagerから伝送単位変換手段cを取得する(ステップS301)。次に、この伝送単位変換手段cに対応する逆変換手段dを構成する(ステップS302)。以下、senderから送られてくる動画像データが尽きると判定される(ステップS306)まで、以下の処理を行う。すなわち、伝送単位変換手段cによって変換された動画像データを受信する(ステップS303)。次に上記受信された動画像データを逆変換手段dによって逆変換する(ステップS304)。最後に、この逆変換された動画像データを、ディスプレイへの表示やディスクへの格納など、receiverが任意に設定した手段を用いて処理を行う(ステップS305)。

【0011】以上において、例えば伝送単位は動画像のフレームであり、伝送単位変換手段cは、所定の長さのビット列と、このビット列を用いてフレーム中一般に複数箇所のビット列を反転させたり並べ替えたりするような、比較的軽微な演算の組み合わせとして構成される。この場合、伝送単位逆変換手段dの構成は容易に実現される。ここで、上記伝送単位変換手段cは所定の認証手段によって保護されており、図3中のステップS301における伝送単位変換手段cの取得時にreceiverの認証を行うことにより、不正な要求に対する変換手段の取得を拒否することで実現されている。以上によれば、伝送単位変換手段cの配付範囲をsenderが認めた範囲に制限することができ、第三者によって被変換データが盗聴された場合であっても、伝送単位変換手段cの強さに応じて解読を防ぐことが可能である。また伝送単位変換手段cとしては、必ずしも高度な暗号化手段を用いる必要はなく、秘話機能を低コストかつ低負荷で実現することが可能である。

【0012】次に第2の実施の形態について説明する。上記第1の実施の形態において、動画像が可変長符号化\*

\*方式によって符号化されている場合には、さらに低コスト化を実現することが可能である。すなわち可変長符号化方式においては、個々の動画像フレームや一組の連続する動画像フレーム列など符号化単位毎に、その先頭部分を伝送単位変換手段cによって変換すれば、この伝送単位変換手段cによる変換が行われていない後続部分についても解読不能になることによる。この場合、例えば伝送単位変換手段cとして上記第1の実施の形態におけるビット列を、所定の乱数の系列を生成するアルゴリズムに従って随時生成するものとすれば、受信側における伝送単位逆変換手段dの構成は容易であり、かつ符号化単位毎に異なる変換がなされるため、仮に第三者によって数フレームの解読がなされたとしても、他の部分については安全性を確保することが可能である。

【0013】尚、上述した各実施の形態においては動画像データを伝送する場合について説明したが他の大容量のデータを伝送する場合であってもよい。

【0014】

【発明の効果】以上説明したように、本発明によれば、動画像データ等の大容量のデータを伝送する場合における秘話機能を低コストで実現することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すブロック図である。

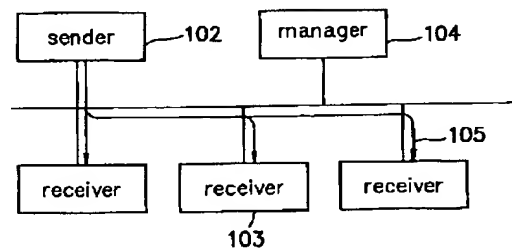
【図2】送信側が動画フレームの送信を行う手順を示すフローチャートである。

【図3】受信側が動画フレームの受信を行う手順を示すフローチャートである。

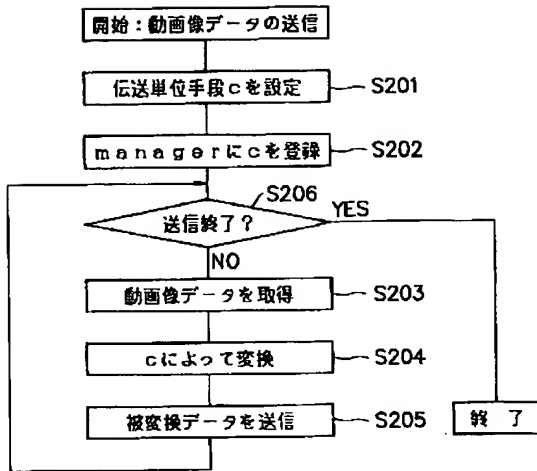
【符号の説明】

101 コンピュータネットワーク  
102 送信端末  
103 受信端末  
104 管理端末  
105

【図1】



【図2】



【図3】

